
GFI MailSecurity deployment strategies

Which operating mode(s) to use in your network environment

GFI MailSecurity can be deployed as an SMTP gateway or as a VS API version for Exchange 2000/2003. This white paper describes each operating mode and helps you decide which to deploy and whether you should deploy both.

Introduction

GFI MailSecurity can be deployed in 2 operating modes: Either as an SMTP gateway or as a VS API version for Exchange 2000/2003. It can be used in 3 ways, either by using one of these modes or by using both in tandem. This paper describes the GFI MailSecurity operating modes in detail and helps you choose the best way to deploy GFI MailSecurity on your network.

Introduction.....	2
Why use both VS API and SMTP gateway modes?	2
About GFI MailSecurity SMTP gateway mode.....	2
GFI MailSecurity VS API Exchange 2000/2003 mode	3
How to deploy GFI MailSecurity	4
GFI MailEssentials & GFI MailSecurity running on the same machine.....	6
About GFI	7

Why use both VS API and SMTP gateway modes?

GFI MailSecurity is the only email content security package to support both an SMTP gateway mode and a VS API mode. For optimum security, we recommend deploying both. This is because both operating modes have unique capabilities that enable you to ensure better security for your network and mail server:

In SMTP gateway mode, GFI MailSecurity checks all inbound and outbound mail before this reaches your mail server. For GFI MailSecurity to do this, you must install it in front of your mail server (or on the Exchange Server if you have Exchange 2000/2003). In VS API mode, GFI MailSecurity is installed on your Exchange 2000/2003 Server and checks inbound, outbound AND internal mail, using the Microsoft VS API interface.

If possible, you should deploy both versions. For administration and performance reasons, it is better to perform the more complex and time-intensive checks at the gateway level. If you were to apply those rules to internal mail, you would end up having to moderate a lot of mail. However, the VS API mode should still be deployed on the Exchange Server, in order to stop a virus outbreak spreading (that could have entered the network via floppy, CD, Web or notebook) or in order to monitor and/or stop internal users using email exploits to siphon off data. You can also use it to prevent unauthorized users from sending executable attachments, which they might use to gain information from users who have more rights on the network.

About GFI MailSecurity SMTP gateway mode

If you wish to install GFI MailSecurity at the perimeter of your network, or if you do not have Microsoft Exchange 2000/2003, you must install GFI MailSecurity in SMTP gateway mode.

In SMTP gateway mode, GFI MailSecurity checks all inbound and outbound mail before this reaches your mail server. To do this, GFI MailSecurity must be the first to receive all mails destined for your mail server and it must be the last "stop" for outbound mail, i.e., mails destined for the Internet. For this to happen, GFI MailSecurity must act as a gateway for all email. This set-up is also known as "Smart host" or "Mail relay" server. Effectively, GFI MailSecurity will act as a mail relay server.

GFI MailSecurity VS API Exchange 2000/2003 mode

If you have Microsoft Exchange 2000/2003, GFI MailSecurity can integrate with Exchange 2000/2003 via the new Microsoft Virus Scanning API (VS API).

What is VS API (Exchange Virus Scanning API) and why use it?

Exchange 2000/2003 provides a new virus scanning API that is implemented at a very low-level in the Exchange store. This allows a virus scanning application to run with high performance and guarantees that the message will be scanned before any client can access a message or attachment. This low-level access facilitates the elimination of viruses such as the Melissa virus.

In addition, VS API reduces scalability issues that can arise when a particular server has a large number of users/mailboxes. VS API's real-time scan allows messages and attachments to be scanned once before delivery, rather than multiple times determined by the number of mailboxes the message is delivered to. This single-instance scanning also helps prevent messages from being rescanned when a message is copied. For more information about VS API, see <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667>.

Limitations of using the VS API Exchange 2000/2003 mode

Although VS API is a recommended way to perform content checking and anti-virus on Exchange 2000/2003, there are a number of limitations that you should be aware of as a system administrator:

1. The Virus Scanning API only scans information stores. That means that if you have installed GFI MailSecurity for Exchange 2000/2003 on a front-end server, for example, no mail will be scanned, because mail is not being stored on the front-end server. In this case, you need to use GFI MailSecurity in SMTP gateway mode.
2. You need to be more careful with applying attachment rules since these might affect internal traffic; attachment rules that are too stringent can result in too much quarantined mail. Also, MAPI applications running on Exchange might be using .vbs or .exe files.
3. Outgoing mails that have been approved need to be resent by the user. For example, if an executable is quarantined and approved, the user will receive a message saying that he/she has 24 hours to resend that executable. The reason for this is that the recipient of

the message is not always known with 100% certainty in VS API mode.

4. In VS API mode, mail is processed in parts. The Exchange VS API interface passes mails to GFI MailSecurity per message part, i.e., the body, attachment 1, attachment 2, etc. This means that message parts are quarantined, not whole messages. Therefore, all rules are applied to a message part. For example, you cannot delete an entire mail if it has a particular content, but only the message part containing that content.
5. In VS API mode, some performance decrease will occur in mail delivery. This is inevitable as all mail has to be checked before the user accesses it. Typically, the delay is approximately 1 second or less, but a mail with a large 15 megabyte attachment, for example, might take more time to scan. Every VS API-based anti-virus solution will suffer from this performance decrease, although of course the less checks are done, the less performance decrease there will be.

Comparison between SMTP Gateway mode and VS API mode

	SMTP gateway	VS API
Scans internal mail	No	Yes
Scans inbound/outbound mail	Yes	Yes
Requires Windows 2000/XP/2003*	Yes (*)	Yes
Requires Active Directory	No	Yes
Requires Exchange 2000/2003	No	Yes
Mail processed in parts	No	Yes
Can run on same machine as GFI MailEssentials	Yes	Yes
Can run if you have Exchange 5.5	Yes	No
Can run if you have Notes or SMTP server	Yes	No
Can run in DMZ or as mail relay	Yes	No
Ticketing system needed **	No	Yes
100% Inbound/internal mail detection***	Yes	No

* - Only on gateway

** - SMTP gateway version has more information about the email, and can therefore quarantine outbound mail without the need for a ticketing system.

*** - SMTP gateway version has more information about the email and can therefore better determine if it is an inbound or an outbound mail.

How to deploy GFI MailSecurity

Deployment option 1

If you have a smaller Exchange 2000/2003 network, and do not want to have a separate mail

relay in the DMZ, use VS API mode only; or if you prefer Gateway mode only.

Smaller networks (eg., Small Business Server)



Rule Set

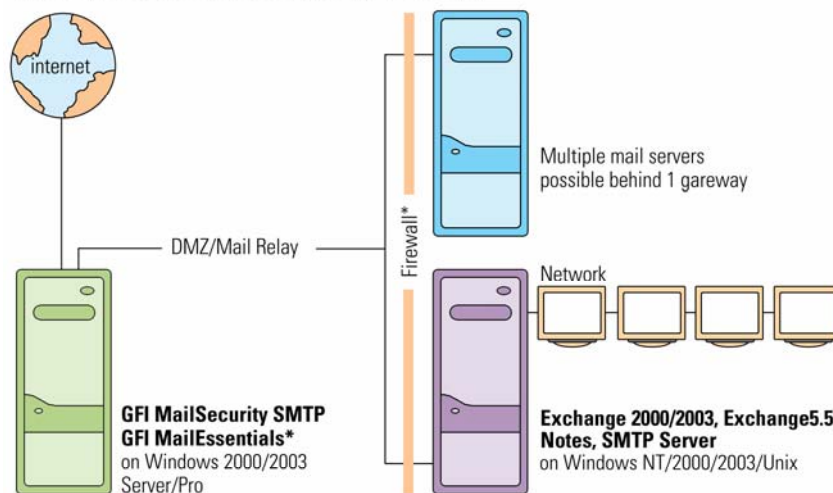
Quarantine inbound & outbound suspicious attachments
 Inbound & outbound and internal virus checking
 Exploit and HTML threats engines and Trojan & Executable Scanner enabled

*optional

Deployment option 2

If you do not have Exchange 2000/2003, deploy GFI MailSecurity in SMTP Gateway mode. So if you have Exchange 5.5, Lotus Notes or another SMTP/POP3 server, you must use SMTP gateway mode.

NT Networks and Windows 2000/2003 networks where GFI MailSecurity does not have to secure internal network



Rule Set

Quarantine inbound & outbound suspicious attachments
 Inbound & outbound and internal virus checking
 Exploit and HTML threats engines and Trojan & Executable Scanner enabled

*optional

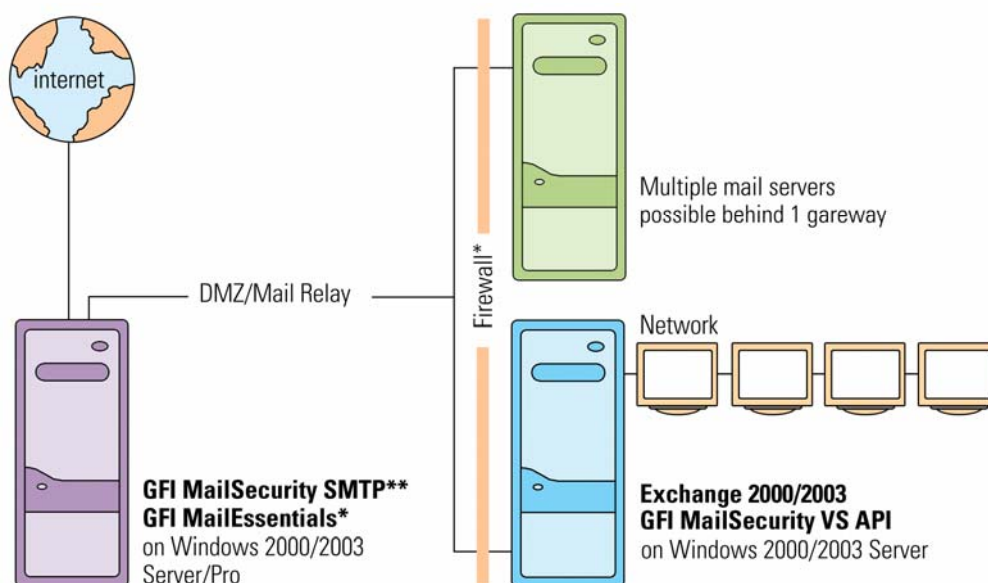
Deployment option 3

If you have a larger network with one or more Exchange 2000/2003 servers, we recommend you deploy GFI MailSecurity both on the Exchange 2000/2003 machine in VS API mode, as well as at the perimeter of your network in SMTP Gateway mode. This is the ideal deployment scenario: the main advantage of this deployment is that you can have stricter rules on inbound and outbound mail, and less strict rules on internal mail.

Larger Windows 2000/2003 networks

Ideal Situation - Deploy both!

1. Use gateway on DMZ to stop threats at the gateway and control what data leaves your company
2. Use VS API to control internal virus outbreaks



Rule Set

Quarantine inbound & outbound suspicious attachments
Inbound & outbound and internal virus checking
Exploit and HTML threats engines and
Trojan & Executable Scanner enabled

Rule Set

Internal virus checking

*optional

** this set-up increases maintenance charge to 30% to cover extra virus engine license

GFI MailEssentials & GFI MailSecurity running on the same machine

GFI Mail essentials and GFI MailSecurity are companion products and can easily run on the same machine. GFI Mail essentials adds essential email tools to your Exchange Server

including anti-spam, disclaimers, mail archiving, Internet mail reporting, server-based auto replies and POP3 downloading. Special bundle pricing applies when GFI MailSecurity and GFI MailEssentials are purchased together.

About GFI

GFI is a leading provider of network security, content security and messaging software. Key products include the GFI FAXmaker fax connector for Exchange and fax server for networks; GFI MailSecurity email content/exploit checking and anti-virus software; GFI MailEssentials server-based anti-spam software; GFI LANguard Network Security Scanner (N.S.S.) security scanning and patch management software; GFI Network Server Monitor that automatically sends alerts, and corrects network and server issues; GFI LANguard Security Event Log Monitor (S.E.L.M.) that performs event log based intrusion detection and network-wide event log management; and GFI LANguard Portable Storage Control that enables network-wide control of removable media. Clients include Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, the US IRS, and the USAF. GFI has offices in the US, the UK, Germany, Cyprus, Romania, Australia and Malta, and operates through a worldwide network of distributors. GFI is a Microsoft Gold Certified Partner and has won the Microsoft Fusion (GEM) Packaged Application Partner of the Year award. For more information about GFI, visit <http://www.gfi.com>.

© 2005 GFI Software Ltd. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

